

Listing of Claims:

Claim 1 (previously presented): A method for propagating filters to an upstream device comprising:

generating and installing a filter at a first network device;

sending information on said filter to a second network device located upstream from said first network device;

requesting said second network device to install a filter so that data is filtered closer to a source of said data;

sending routing information from said first network device to said second network device so that the filter installed on said second network device filters traffic forwarded to said first network device without filtering traffic to other downstream nodes; and

analyzing new data received from said second network device at said first network device and sending filter information to said second network device based on the analyzed data so that said second network device can refine the filter installed thereon.

Claim 2 (original): The method of claim 1 wherein generating a filter at a first network device comprises automatically generating said filter based on network flow entering the device.

Claim 3 (original): The method of claim 1 further comprising receiving information based on monitored network flow and removing said filter from the first network device when the network flow requiring said filter is no longer present.

Claim 4 (original): The method of claim 3 further comprising requesting said upstream device to remove said filter.

Claim 5 (original): The method of claim 1 further comprising refining said filter at said first network device based on said monitored network flow.

Claim 6 (original): The method of claim 5 further comprising requesting the upstream network device to refine said filter.

Claim 7 (previously presented): The method of claim 1 wherein generating a filter comprises detecting potentially harmful network flows and generating a filter to prevent packets corresponding to said detected potentially harmful network flows from passing through said second network device.

Claim 8 (original): The method of claim 7 wherein generating filters further comprises classifying network flow based on a source device sending a packet.

Claim 9 (original): The method of claim 8 wherein the network flow is classified based on an address of the source device.

Claim 10 (original): The method of claim 1 wherein generating filters comprises analyzing network flow entering said first network device.

Claim 11 (original): The method of claim 10 wherein analyzing said network flow is performed by software.

Claim 12 (original): The method of claim 10 comprising selecting a class of network flows to analyze based on previously analyzed network flows.

Claim 13 (previously presented): A computer program product for propagating a filter to an upstream device, comprising:

- code that generates and installs a filter at a first network device;
- code that sends information on said filter to a second network device located upstream from said first network device;
- code that requests said second network device to install said filter;
- code that sends routing information from the first network device to the second network device so that the filter installed on the second network device filters traffic forwarded to the first network device without filtering traffic to other downstream nodes;
- code that analyzes new data received at the first network device from the second network device and sends filter information to the second network device based on the analyzed data so that the second network device can refine the filter installed thereon; and
- a computer-readable storage medium for storing the codes.

Claim 14 (original): The computer program product of claim 13 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave.

Claim 15 (original): The computer program product of claim 13 wherein the code that generates said filter comprises code that analyzes network flows and detects potentially harmful network flows.

Claim 16 (original): The computer program product of claim 13 further comprising code that removes said filter from the first network device when no longer required.

Claim 17 (original): The computer program product of claim 13 further comprising code that requests said upstream device to remove said filter.

Claim 18 (previously presented): A system for propagating filters to an upstream device, comprising:

- means for generating and installing a filter at a first network device;
- means for sending information on said filter to a second network device located upstream from said first network device;
- means for requesting said second network device to install said filter;
- means for sending routing information from the first network device to the second network device so that the filter installed on the second network device filters traffic forwarded to the first network device without filtering traffic to other downstream nodes; and
- means for analyzing new data received at the first network device from the second network device and sending filter information to the second network device based on the analyzed data so that the second network device can refine the filter installed thereon

Claim 19 (previously presented): A method for installing filters on connected network devices, comprising:

- analyzing network flows received at a first network device having a filter installed thereon;
- generating a filter at a second network device based on said analyzed flows;
- propagating said filter from the second network device to the first network device;
- generating filter statistics at the second network device;
- sending said filter statistics to the first network device; and

utilizing a filter propagation protocol to exchange information directly between the first and second network devices to refine said filter.

Claim 20 (original): The method of claim 19 wherein propagating said filter comprises propagating filter information upstream such that said filter is positioned closer to a source of said flows.

Claim 21 (canceled).

Claim 22 (previously presented): The method of claim 1 wherein receiving filter information comprises using a filter propagation protocol.

Claim 23 (original): The method of claim 22 wherein the filter propagation protocol is operable to create, remove, or modify existing filters.

Claim 24 (original): The method of claim 22 wherein the filter propagation protocol uses negative routing.

Claim 25 (canceled).

Claim 26 (previously presented): The method of claim 1 wherein said flow information includes a packet and byte count of packets received and dropped at the upstream device.

Claim 27 (canceled).

Claim 28 (canceled).

Claim 29 (previously presented): The method of claim 19 further comprising reinstalling said filter at predefined intervals to extend the lifetime of said filter and return packet and byte count statistics for said filter.

Claim 30 (previously presented): The method of claim 1 further comprising:

- classifying network flow received at the second network device;
- performing a lookup in a flow cache;
- building a new entry in the flow cache if the network flow is not found;
- generating a flow record based on the network flow;
- analyzing the flow record along with previous generated flow records;
- modifying said filter installed at the second network device based on said analyzed flow records; and
- transmitting data from the second network device to the first network device so that the first network device can modify the filter installed thereon.

Claim 31 (previously presented): The method of claim 30 wherein classifying network flow comprises classifying said network flow based on an access control list.

Claim 32 (previously presented): The method of claim 30 wherein classifying network flow is performed on only a limited number of packets received in said network flow.

Claim 33 (previously presented): The method of claim 30 wherein analyzing said flow records comprises analyzing aggregate summary records.

Claim 34 (previously presented): The method of claim 30 wherein analyzing said flow records comprises monitoring statistics associated with said filter installed on the second network device.

Claim 35 (previously presented): The method of claim 1 further comprising utilizing reverse path forwarding at said second network device.

Claim 36 (previously presented): The method of claim 1 wherein a filter propagation protocol is utilized to exchange information between said first and second network devices and modify said filters installed on said network devices.

Claim 37 (previously presented): The method of claim 1 wherein the first network device is a firewall and the second network device is a router.

Claim 38 (previously presented): The method of claim 1 wherein sending routing information from said first network device to said second network device comprises utilizing an inter-router filter propagation protocol.

Claim 39 (previously presented): The method of claim 38 wherein the filter information is automatically propagated upstream to filter data close to the source of the data.

Claim 40 (previously presented): The method of claim 1 further comprising detecting harmful network flows using a network directory and flow analyzer.

Claim 41 (previously presented): The method of claim 1 wherein the first network device is an enterprise switch and the second network device is a router.

Claim 42 (previously presented): The method of claim 1 further comprising sending filter information from the second network device to the first network device.

Claim 43 (previously presented): The method of claim 42 wherein sending said filter information comprises limiting the number of filters that the first network device can request the second network device to install.

Claim 44 (previously presented): The method of claim 42 wherein sending said filter information comprises requesting the first network device to install filters.